UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Director
Bureau of Consumer Protection

December 9, 2009

Via Electronic Filing

Marlene H. Dortch, Esquire
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Comments - NBP Public Notice #21
GN Docket Nos. 09-47, 09-51, and 09-137

Dear Ms. Dortch:

The Federal Trade Commission (FTC) staff appreciates this opportunity to comment on the Federal Communications Commission's (FCC) Notice of Inquiry on how broadband and portability of data relate to cloud computing, transparency, identity, and privacy. We believe that strong privacy and data security protections for consumers are critical as the FCC considers technologies such as cloud computing and identity management in implementing a national broadband plan.

The FTC has made privacy one of its highest consumer protection priorities for more than a decade.[1] The FTC has worked to address privacy issues through law enforcement, regulation, policy initiatives, and consumer and business education. For example, since 2001 the FTC has brought over two dozen law enforcement actions that challenged businesses that allegedly failed to adequately protect consumers' personal information.[2] These cases emphasize the importance of protecting consumers against common security threats and the need for businesses to evaluate their security procedures on an ongoing basis. In addition, the FTC established the Division of Privacy and Identity Protection in 2006, which is devoted exclusively to privacy-related issues. Over the years, the FTC's goals in the privacy arena have remained constant: To protect consumers' personal information and to ensure that consumers have the confidence to take advantage of the many benefits offered by the ever-changing marketplace.

The FTC staff presently is examining "cloud computing" and its privacy and data security implications for consumers. Cloud computing, which is defined broadly as the provision of

---

1 *See generally* FTC, Privacy Initiatives, http://www.ftc.gov/privacy/index.html.

2 *See id.*

Internet-based computer services, allows businesses and consumers to use software and hardware located on remote computer networks operated by third parties. Because cloud computing has the potential to reduce the need for businesses and consumers to purchase, operate, and maintain software and hardware themselves, it may be a less costly way for them to manage, store, and use data. However, the storage of data on remote computers may also raise privacy and security concerns for consumers. For example, the ability of cloud computing services to collect and centrally store increasing amounts of consumer data, combined with the ease with which such centrally stored data may be shared with others, create a risk that larger amounts of data may be used by entities in ways not originally intended or understood by consumers.

The FTC also considers identity management, including authentication and credentialing issues, to be a key part of its privacy and data security program. In 2007, the FTC hosted a workshop that focused on technological and policy requirements for developing better processes to authenticate individual identities.[3] In 2008, the FTC issued a report on Social Security numbers, which encouraged businesses to strengthen the methods used to authenticate new and existing customers in order to protect consumers against identity theft.[4] Finally, the Commission has used its authority under Section 5 of the FTC Act to challenge companies' failure to implement reasonable credentialing programs that resulted in consumer harm.[5] For example, in its case against ChoicePoint, the FTC alleged that the data broker failed to have reasonable procedures to screen prospective subscribers and monitor existing customers; as a result, identity thieves posing as legitimate businesses were able to access the sensitive personal information of more than 163,000 consumers. In settling with the FTC, the company agreed to pay $10 million in civil penalties – the largest civil penalty in FTC history – and $5 million in consumer redress. In addition, the company agreed to implement procedures to better authenticate and monitor its customers' use of sensitive consumer data.

Currently, the FTC is considering cloud computing and identity management as part of a broader initiative to reexamine various models to promote consumer privacy. The FTC is hosting a series of day-long public roundtable discussions to explore the privacy challenges posed by the vast array of 21st century technologies and business practices that collect and use consumer data.[6] The goal of the roundtables is to determine how best to protect consumer

---

[3] *See* FTC Workshop, *Proof Positive: New Directions for ID Authentication* (April 23-24, 2009), *available at* http://www.ftc.gov/bcp/workshops/proofpositive/index.shtml.

[4] *See* FTC Report, *Security in Numbers: SSNs and ID Theft* (Dec. 2008), *available at* http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf. At the same time, the report recognized that more robust authentication procedures can raise privacy concerns. For example, the report noted that while some businesses collect additional personal information to improve their authentication processes, such increased data collection can have an impact on consumer privacy.

[5] *See, e.g., United States v. Rental Research Svcs.*, No. 09-CV-00524-PJS-JJK (D. Minn. Mar. 5, 2009); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of Reed Elsevier Inc.*, FTC Docket No. C-4226 (July 29, 2008).

[6] More information about the Privacy Roundtables can be found at http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml.

privacy while supporting beneficial uses of the information and technological innovation. The FTC believes that many of the issues raised in the FCC's notice – such as the privacy and data security implications of cloud computing and identity management and whether there is a need for greater protections for consumers – will be addressed through the roundtable discussions as well as through requests for comments and original research.

The first roundtable discussion, held on December 7, 2009, considered the risks and benefits of information collection and use in online and offline contexts, consumer expectations surrounding such practices, behavioral advertising, information brokers, and the adequacy of existing legal and self-regulatory regimes to address privacy interests. The second roundtable, which will be held on January 28, 2010, will focus on how technology affects consumer privacy, including its role in both raising privacy concerns and enhancing privacy protections. The second roundtable will include specific discussions on cloud computing, identity management, mobile computing, and social networking. Details regarding the third and final roundtable, which will take place on March 17, 2010, in Washington, DC, will be announced at a later date.

The FTC staff supports the FCC's decision to consider privacy and data security interests as it contemplates the use of cloud computing and identity management in its development of a broadband plan. We believe that the information gathered at its upcoming privacy roundtables will assist the FCC as it considers consumer privacy in these contexts. The FTC will continue to devote substantial resources to protecting consumers from deceptive or unfair acts or practices in the areas of privacy and data security, and we look forward to working with the FCC on such issues in the future. Accordingly, we recommend that the Broadband Plan recognize the FTC's law enforcement, consumer education, and ongoing policy development efforts in light of its years of experience in online, and offline, consumer protection.

Sincerely,

David C. Vladeck